Determining the Suitability of COTS for Mission Critical Applications

Ronald J. Kohl

AverStar, Inc.
3581 Mar Lu Ridge Road
Jefferson, MD, USA, 21755-7724
kohl@averstar.com

Abstract

Commercial Off The Shelf (COTS) products are being considered for inclusion in ever more complex and critical systems. There are known advantages and risks [1, 4, 5] for considering the use of COTS in complex systems. Yet, given the rigorous needs of Mission Critical systems or subsystems, there have begun to emerge concerns and risks about the suitability of COTS for such applications. This paper identifies some of the characteristics of Mission Critical systems (e.g. reliability, availability, correct functionality) that makes the selection process of COTS products (hardware, software, subsystems, etc) an increasingly important factor in total system lifecycle phases (design, development, acceptance, operations/maintenance and disposal). This paper presents a set of risk areas related to the use of COTS, in general, and specifically for Mission Critical systems, that would assist both the acquisition community as well as the development/integration community in determining the suitability of using COTS in such Mission Critical systems. Then, a set of risk mitigation approaches is identified; some of which have been applied to certain National Aeronautics and Space Administration (NASA) programs. Lastly, a set of steps that could lead to the establishment of a set of procedures, and perhaps even an enterprise policy on if and/or when COTS products are suitable for certain Mission Critical applications.

1 Introduction

Mission Critical System characteristics such as reliability, safety, availability, maintainability, and certification tend to have significant influence on whether or not COTS should be considered for a given application. On the other hand, COTS products traditionally have not been built for use in such Mission Critical applications. This systems needs versus intended product operational envelope poses one of the major challenges to using COTS products in such Mission Critical systems. Once the suitability of COTS has been determined, then it is possible that additional requirements may be placed on the product and/or the product's vendor prior to inclusion in such Mission Critical applications. Or it may be necessary to consider alternative products or approaches if a given vendor is unwilling to comply with Mission Critical product/system requirements. Further, it is possible that certain system requirements and expectations may need to be modified because of the inclusion of COTS products into that system. As COTS products continue to be considered as candidates for inclusion within Mission Critical systems, there will likely be additional risk factors that will be identified, and there will likely be improvements to the impacts of known risks to existing COTS risk factors. The continued pursuit and dissemination of such COTS risk factors will influence how both acquirers and suppliers decide if and/or when to use COTS products. Ongoing monitoring of this technology area, including both benefits attained and risks identified, seems to be warranted. In addition, validation of the mitigation techniques proposed in this paper is warranted, along with collecting lessons learned from projects, which may be experiencing such impacts, and those that may have identified additional mitigation techniques.

2 Background

Trends in both government and industry are to use COTS products more and more because there are recognized advantages: reduced development cost, large user base, reduced maintenance, etc. This trend seems to be increasing with no end in sight.

Yet, Mission Critical systems and applications continue to have ever more stringent and rigorous requirements for certain characteristics of the system or application. And there is every reason to expect that such Mission Critical systems will increase in number, complexity, and stringency.

Determining the suitability of any COTS products for such applications and systems requires efforts and analyses that may not be fully appreciated, understood, or implemented in many organizations. This is true of acquiring organizations as well as of supplying organizations.

Further more, there can be non-engineering pressures to use COTS products (Department of Defense's (DoD) Acquisition Reform, U.S. Government's legislation on Information Technology Management Reform Act (Clinger-Cohen), DoD's transition out of Mil-Stds to commercial standards (Perry memo), etc).

Paper presented at the RTO IST Symposium on "Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS"", held in Brussels, Belgium, 3-5 April 2000, and published in RTO MP-48.

3 What are the differences in Mission Critical systems?

There is no agreed upon definition of Mission Critical systems. The intent is that such Mission Critical systems are more important than other systems, based on the perspective of a set of stakeholders. The problem is that more important tends to be an ill-defined characteristic. For the purposes of this paper, Mission Critical System is defined as "any system critical to success of an enterprise or a project". Mission critical systems have more rigorous and stringent requirements than less critical systems. These requirements usually have to do with quality and performance characteristics. Requirements in the area of availability, reliability, security, and safety are usually of higher priority for Mission Critical systems, and pose greater impacts on the subsystems, components, and elements of such systems. Financial systems, such as International Bank funds transfer, may have less complex functionality but the loss of availability, even for a few seconds, can have significant mission impacts to entire enterprises. Military facilities have security requirements that are critical to the mission of such secured facilities and enterprises. And human-based space programs have safety requirements that cannot be compromised.

In addition, Mission Critical systems tend to have more demanding performance requirements. It is not unusual for Mission Critical systems to have real-time, throughput, access, and response requirements that are far more difficult to satisfy and verify, especially via COTS products. Chemical processing plants have the need to monitor sensors many times per second, to ensure safety. Space propulsion systems have a need to monitor sensors and command effectors, many times per second, to correctly control launch vehicles and orbiting platforms. Security systems need to access restricted and protected databases in microseconds, and to disseminate the information from those accesses, over large networks in a matter of seconds, or less.

One last area of relevance to Mission Critical systems is the need for more stringent Verification and Validation efforts and possibly even product certification. NASA's Space Shuttle Program (SSP) requires software certification by both the developer and the independent verifier. Security systems also require product certification.

The above is intended to provide examples of Mission Critical requirements that are either unique to or more critical, none of which can be compromised, no matter what the solution's composition.

4 What are the risks of using COTS products in Mission Critical systems?

There is a growing body of information [1, 4, 5] that has identified risk areas when considering COTS products. These include functionality of the product, operational utilization, quality and reliability, maintenance costs, product volatility, and vendor viability.

These risk areas need to be assessed, and when appropriate, mitigated no matter what type of system that contains them.

However, Mission Critical places even higher demands on COTS products and vendors. Some examples are:

- It may be undesirable or even unacceptable for a COTS product to contain Dormant Code [3], the COTS product functionality for which there is no system requirement. Dormant Code can have technical, cost, schedule, and even legal ramifications that might disqualify a given COTS product.
- It may be mandatory to have insights into the product development processes to understand the likelihood of a quality product upon delivery. It may even be an acquisition requirement for all suppliers (from prime to subcontractors to vendors) to be ISO 9000 or SEI CMM Level 3.
- It may be necessary to have access to source code, in order to understand functionality and testability of a given COTS product.
- For long-lived systems, it may be necessary to have access to product information (source code, design documents, test scripts, etc) since a given version of a product may need to be operational for many years. This may require such approaches as source code escrow or third party maintenance agreements.
- Vendors may be required to produce or obtain certification of their COTS product, which often incurs legal and financial implications.

5 An overview of what should be done

The first step is to fully understand the expectations, desires and characteristics of the system or application to be developed, and to determine the priority of each of these needs. This will support the establishment of a critical shopping list as the system supplier ventures into the commercial component marketplace.

Almost in parallel, an understanding and insight into the availability and characteristics of the COTS products that could be solution candidates, needs to begin to be developed. Furthermore, insights into vendor business viability and reputation need to be captured and then monitored.

Then there must be an iterative process of requirements specification and candidate COTS solution evaluations. As systems requirements mature and as COTS product knowledge increases and improves, it will likely be necessary to revisit the matches and mismatches between requirements and COTS capabilities.

Additionally, if system acceptance requirements such as Independent Verification and Validation or Operational Certification are required, then determining the ability of COTS products, and their vendors to undergo the rigors of complying with such requirements, becomes a significant factor in the earliest phases of the system's lifecycle.

6 Specifically, what are the next steps?

1. Ensure that Mission Critical systems are not over specified. Be sure that only those components and subsystems of a given system that need to be very important are subject to the appropriate and more stringent Mission Critical requirements. As systems requirements mature and evolve, it is critical that these requirements be continually compared against COTS product capabilities.

2. Determine the capabilities of COTS products, and where appropriate the viability of their vendors. This must be performed early and often. It could be necessary to establish a commercial product market watch role to ensure that the COTS marketplace, the vendors in that marketplace, and the products produced by those vendors meet the system requirements.

3. Understand the operational profiles of the system to ensure that any operational concepts for COTS products, as envisioned by the vendor, are consistent with the operational profiles of the end system. This can be a major area for significant disconnect if not addressed early and revisited often.

4. Determine if there are additional approaches to determine the compliance of COTS products with Mission Critical requirements. Such approaches as additional testing, vendor certification, and third party product certification may be required.

5. Establish positive relationships with the COTS vendors to promote good business dealings. Such positive business relationships can ease or improve negotiations with COTS vendors, where appropriate, for access to product and process information not normally provided by such vendors (they may not necessarily say no!)

6. Understand alternative COTS products. This requires knowledge of the marketplace, the vendors and products in that marketplace and the products that are emerging into the marketplace. By knowing the full range of candidate solution components, there is reduced risk that the final solution will satisfy the full spectrum of systems requirements.

7 An example

The United State's NASA SSP recently selected a commercial GPS system (a military version of a commercial GPS system) to replace the onboard TACANs for navigation functionality. A test/acceptance program was implemented, including test flights onboard the Space Shuttle Orbiter. A respected vendor was selected from candidates and SSP began to perform a set of analyses and tests to validate the capabilities and quality of this product. In spite of what was considered the correct processes to satisfy SSP's expectations of this GPS subsystem, an on-orbit problem occurred during the first test flight on Shuttle Mission STS-91, in 1999 [2].

The nature of the problem lied in an interface between the Onboard Flight Software (FSW) and the GPS Receiver subsystem. Certain problems, not fully understood by the SSP, manifested themselves during STS-91, leading to Nav state divergence that eventually manifested itself in loss of communications between the Orbiter and the ground. As a consequence of this problem, NASA has reverted to the TACANs, has improved the interface between the FSW and the GPS subsystem (more protection), and has implemented a variety of more stringent analyses and process improvements.

What were the assumptions that were made to support the adoption of the commercial GPS receiver?

- Reduced costs to SSP.
- Leverage from military experience and testing of GPS Receiver subsystem.
- Adoption of new technology in reduced time (obsolescence was a factor).
- Intense Black Box testing would satisfy V&V requirements and expose any hidden problems.

What were the risks/problems encounter?

- Operating environment/profile was different.
- Insufficient Systems Engineering across all aspects of the GPS system, especially the firmware.
- Process rigors of SSP were not satisfied by the GPS Receiver vendor.
- Lack of insight into GPS Receiver design.
- Lack of GPS math model.
- Declining vendor knowledge on the GPS Receiver product line.

What were the lessons learned or changes made by SSP?

- COTS/MOTS should not be considered a silver bullet
- Thorough Systems Engineering, early and often, remains critically important.
- Relying on Black Box testing has limits and may be insufficient.
- Lack of insights into product designs can lead to unknown problems.
- COTS vendors should be involved early and across the lifecycle.

8 What future steps could be considered?

1. Validate the above set of practices by industry and government practitioners.
2. Contact (survey, interview, etc) current programs that have Mission Critical components and determine if they are considering COTS products. If they are, determine how they select COTS products.
3. Contact researchers (industry, government, and academia) to determine areas suitable for long term study/analysis/research.
4. Maintain an ongoing monitoring of these practices and the users of them, to reassess the validity of them and to identify new practices for consideration.

9 Conclusions

The use of COTS products in Mission Critical systems is an emerging trend, which requires sound engineering practices. Not all of these practices are fully understood or mature, yet. As the practices suggested in this paper are implemented, they will be improved and new ones will emerge. There is much to learn about effectively using COTS products, across the total system lifecycle. Moreover, there are additional risks and mitigation techniques that affect Mission Critical systems, some of which have yet to be identified. Further validation of the practices suggested here and the emergence of new practices will improve the ability of systems developers to incorporate COTS products while still satisfying the critical demands of large, complex systems.

References

[1] J. Clapp, A. Tabb, “A Management Guide to Software Maintenance in COTS-Based Systems”, Mitre Corp, Mitre Paper MP 98B0000069, Nov. 1998.

[2] J. Hutchins, “Shuttle GPS Upgrade, COTS/MOTS Issues and Lessons Learned”, Proceedings, ATWG Fall Conference, 1999.

[3] R. Kohl, “When Requirements are not isomorphic to COTS Functionality: “‘Dormant Code’ within a COTS product”, Proceedings INCOSE Symposium, July, 1998.

[4] D. Reifer, T. Ragan, G.E. Kalb, “COTS Software Management: Taming the Beast”.

[5] SEI, “COTS-Based Systems (CBS) Initiative”, at http://www.sei.cmu.edu/cbs/index.html.